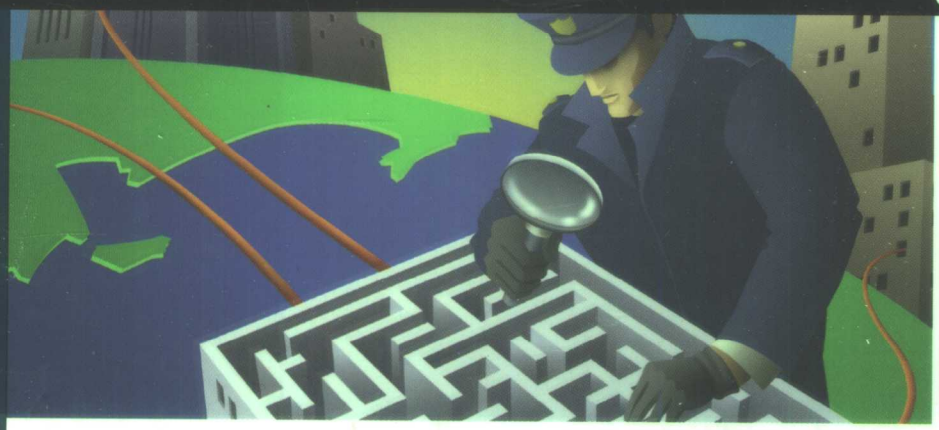
CISCO SYSTEMS

CQS



Managing Cisco® Network Security

Prepare for the Cisco Security Specialist certification with the Official MCNS Coursebook

ciscopress.com

Michael Wenstrom

About the Author

Mike Wenstrom is an education specialist at Cisco Systems, Inc., where he designs, develops, and delivers training on Cisco's virtual private network and network security products.

Mike has chosen a career in training and instruction to help people improve their knowledge and skills in communications technologies. He especially enjoys translating complex technical subjects into an easy-to-understand form. Mike has over 18 years of experience in many facets of technical training, having been an instructional designer, course developer, technical instructor, and project manager.

While a 21-year resident of Silicon Valley, Mike worked for Cisco Systems, Aspect Communications, Siemens, IBM, ROLM, Tymnet, NCR, and the U.S. Navy. He currently develops training for and teaches Cisco's VPN and network security products in Austin, Texas, where he resides with his wife and daughter. He graduated from Western Illinois University with a BA degree. He has an AS degree in electronics technology and is a CCNA.

About the Contributing Authors

J.T. Agnello has been a systems administrator in Austin, Texas, for the past 15 years, performing systems and network administration and management for companies that range in size from small-to-medium businesses (SMB) to large enterprises such as Sematech, Schlumberger, IBM, and others. He has been writing technical training courses for the past three years, producing courses that cover such topics as systems, network, security, and database management, for companies such as Tivoli Systems (an IBM company) and Pervasive Software.

Scott Morris is an instructor/consultant for Mentor Technologies, Inc. (formerly Chesapeake Computer Consultants). He has worked in many different areas involving computers and networks. Through Novell certifications, Microsoft certifications, and Cisco certifications, Scott has covered many areas, and he continues to enhance his credentials (and to relieve boredom).

Regarding Cisco pursuits, Scott is a Cisco Certified Systems Instructor (CCSI), CCIE #4713 in Routing and Switching, a CCDP in Routing and Switching, and a CCNA in WAN Switching. Scott has passed the CCIE written exams for the ISP-Dial and Design tracks, and he currently uses his little spare time to work on his next CCIE lab exam (ISP-Dial first!). Scott primarily teaches Cisco Internetwork Troubleshooting (CIT), but he tends to pick up courses on brand-new technology just for fun.

Cary A. Riddock has been a network engineer for a large Central Florida healthcare management company for the past year. His duties include monitoring the corporate LAN/WAN and troubleshooting connectivity-related problems. Currently, he is working on a system that will allow corporate executives to access private intranet applications via the public Internet utilizing PKI and token card–based authentication technology. Cary holds the following certifications: MCSE, CCNA, CCDA, CCDP, and CCA.

About the Technical Reviewers

This book's reviewers contributed their considerable practical, hands-on expertise to the entire development process for *Managing Cisco Network Security.*

Richard Benoit serves as the Network and Technology Project Manager for an international entertainment conglomerate headquartered in Orlando, Florida. Currently, his work focus is on enterprise network design, management, and security issues. Formerly, as a consultant, he worked with many customers in the design, implementation, and support of large-scale network solutions. His network certifications include CCNP + Security, CCDA, and Microsoft MCSE. He holds a BS in Management Systems from the Milwaukee School of Engineering.

Doug MacBeth is an IOS documentation manager at Cisco Systems, Inc. He has more than 15 years of experience in technical documentation and has worked for Cisco Systems since 1993. While at Cisco, Doug has been an Editor and a Project Leader for the Cisco IOS documentation set. Doug lives in San Jose, California. He holds a Bachelor's Degree in Technical and Business Communications from San Jose State University.

Doug McKillip, P.E., CCIE #1851, is an independent consultant specializing in Cisco Certified Training in association with Global Knowledge. He has more than 12 years of experience in computer networking, and for the past eight years, he has been actively involved in security and firewalls. Doug provided both instructional and technical assistance during the initial deployment of the MCNS version 1.0 training class, and he has been the Lead Instructor and Course Director for Global Knowledge, a Training Parter of Cisco Systems. Doug holds Bachelor's and Master's Degrees in Chemical Engineering from MIT and a Master's Degree in Computer Science from the University of Delaware. He resides in Wilmington, Delaware.

Hank Mauldin is a Consulting Engineer for Cisco Systems, Inc., working for the Office of the CTO. He has worked with Cisco for several years, evaluating and designing data networks. His areas of expertise include IP routing protocols, quality of service, and network security. Hank currently is Program Manager for Cisco Network Designer, which is a network design tool. Prior to joining Cisco, he worked for several different system integrators. He has more than 15 years of data networking experience. Hank resides in San Diego, California. He holds a Master's Degree in Information System Technology from George Washington University.

Acknowledgments

The MCNS course was a community project with many contributors inside and outside Cisco, including Cisco course developers, course editors, and instructors. Although I was the primary course developer for the MCNS course, I would like to acknowledge the important efforts of others who made the course a success: Tom O'Hara, Sean Coville, and Bob Martinez as contributing course developers; Matt Lyons, Franjo Majstor, and Kevin Calkins as Cisco instructors, Hank Mauldin and Chris Lonvick as course consultants and architects; Doug McKillip as the key Cisco Learning Partner instructor; Brian Adams and Deborah Lewis as course editors; and Chris Berriman as the manager for the initial MCNS project.

Developing the MCNS book was a difficult yet rewarding project. I would like to acknowledge my manager, Rick Stiffler, and my workmates in the security training group, who tolerantly put up with the many times I came to work after toiling over the book until 2 the previous night. I would also like to acknowledge the Cisco Press staff, who tried to keep me on track to bring the book to a close. Kitty Jarrett and Brett Bartow deserve special commendation for patiently working with me and the other authors throughout the project. I appreciate the significant contributions made by the technical reviewers, and I thank the other authors who made this book a success.

Foreword

Managing Cisco Network Security presents in book format all the topics covered in the challenging instructor-led certification preparation course of the same name. MCNS teaches you the knowledge and skills needed to install, configure, operate, manage, and verify Cisco network security products and Cisco IOS software security features in IP networks. You will learn how to identify network security threats, secure remote dial-in access with CiscoSecure ACS and Cisco IOS AAA features, protect Internet access using Cisco perimeter routers and PIX Firewalls, and implement secure VPNs with IPSec. Whether you are preparing for the Cisco specialization in security or are seeking to gain a practical understanding of Cisco network security solutions, you will benefit from the information presented in this book.

Cisco and Cisco Press present this material in text-based format to provide another learning vehicle for our customers and the broader user community in general. Although a publication does not duplicate the instructor-led environment, we acknowledge that not everyone responds in the same way to the same delivery mechanism. It is our intent that presenting this material via a Cisco Press publication will enhance the transfer of knowledge to a broad audience of networking professionals.

Cisco Press will present existing and future courses through these course books to help achieve Cisco Internet Learning Solutions Group's principal objectives: to educate the Cisco community of networking professionals and to enable that community to build and maintain reliable, scalable networks. The Cisco Career Certifications and classes that support these certifications are directed at meeting these objectives through a disciplined approach to progressive learning. The books Cisco Press creates in partnership with Cisco Systems will meet the same standards for content quality demanded of our courses and certifications. It is our intent that you will find this and subsequent Cisco Press certification and training publications of value as you build your networking knowledge base.

Thomas M. Kelly
Vice President, Internet Learning Solutions Group
Cisco Systems, Inc.
July 2000

Preface

Computer and network security have become front-page news due to the prevalence of attacks and the realization that the Internet revolution is here to stay and is the key to prosperity of individuals and countries. Leaders of nations and companies worldwide have been forced to pay attention to the urgent need for network security. Many have realized that their networks lack even basic security measures and that there are not enough network professionals trained to implement network security. Yet network security seems to be a complex, even esoteric subject that defies understanding by any but the most elite network professionals.

Many of us whose careers are focused on increasing the knowledge and competency level of networking professionals saw the need to create a holistic approach to teaching network security in order to help people get started in better securing their networks. We saw the need to jump-start people into the network security field so that many more people could develop security expertise, thereby increasing network security as a whole. We decided to create a new network security course to address the anticipated need.

Early in 1997, while a developer in Cisco Worldwide Training, I was assigned by my then-manager, Chris Berriman, to develop the Managing Cisco Network Security (MCNS) course. Although nobody had yet requested such a course, our group had the vision to anticipate the eventual exploding need for network security training. I performed an informal survey of competitive offerings and found that no other companies were offering an equivalent course.

The course was intended to provide a survey of Cisco network security technology, balancing breadth of technology offering with depth of coverage on each subject. Hands-on lab exercises would cement concepts and facts. The MCNS project was launched, and a team effort led to the production of the first and subsequent versions.

This book is parallel in content to the MCNS course, yet it is completely rewritten based on extensive research. The need for a comprehensive network security book is especially strong today. This book addresses the compelling need to educate many more networking professionals and associates on vital network security needs, making network security available and understandable to many more people.

Mike Wenstrom
Cisco Systems, Inc.
August 2000

Introduction

The goal of this book is to help readers implement Cisco-supported network security technologies and design and implement more-secure networks. This book is designed to supplement the MCNS course or act as a standalone reference.

This Book's Audience

The book is written for anyone who wants to learn about Cisco network security features and technologies. The main target audience is networking professionals who need to expand their knowledge beyond routing and switching technologies and improve their ability to install, configure, monitor, and verify Cisco network security products and features. This book assumes that you have a knowledge of Cisco networking equivalent to that required to pass the CCNA certification exam.

The secondary target audience is general users who need to understand network security threats and how to mitigate those threats. This book explains many network security concepts and technologies with a user-friendly approach that should appeal to readers who prefer less-technical manuals.

This Book's Features

This book has a number of unique features that will help you learn and put to work the network security topics covered in this book:

- **Concepts covered**—At the beginning of each chapter is a list of topics covered in that chapter. This provides a reference to the concepts covered and can be used as an advanced organizer.
- **Figures, examples, and tables**—This book contains figures, examples, and tables that present each chapter's content in an easy-to-use form. The figures help explain concepts and software processes, the examples provide examples of commands and output, and the tables present facts such as command syntax with descriptions.
- **Case studies**—The XYZ Company, a hypothetical enterprise, is used in each chapter to anchor configuration examples into a unified whole and to make the examples more realistic. A sample network security policy based on the XYZ Company is used throughout this book as a model of how to implement security policy directives. Case study network examples in many chapters summarize configuration information taught in the chapter based on the XYZ customer environment.
- **Command summaries**—Command summaries are included with each subject instead of in a separate section as a courtesy to you, making it easier to learn and apply the tasks being presented.

- **Chapter summaries**—At the end of each chapter is a summary of the concepts covered in that chapter. It provides a synopsis of the chapter and serves as a study aid.
- **Review questions**—After the summary in each chapter are 10 review questions that reinforce the concepts presented in that chapter. They help you test your understanding before you move on to new concepts. The answers to these questions are provided in Appendix D.
- **References**—After the review questions is a listing of references related to the topics presented in that chapter. They help you extend your knowledge beyond what is covered in the chapter.

Conventions Used in This Book

This book uses the following conventions:

- Important or new terms are *italicized.*
- All code examples appear in `monospace` type, and parts of code use the following conventions:
  - Commands and keywords are in **bold** type.
  - Arguments, which are placeholders for values the user inputs, appear in *italics.*
  - Square brackets ([ ]) indicate optional keywords or arguments.
  - Braces ({ }) indicate required choices.
  - Vertical bars (|) are used to separate required choices.

This Book's Organization

This book is divided into seven parts, including 18 chapters and four appendixes.

Part I: Establishing Network Security Policy

Chapter 1, "Evaluating Network Security Threats," answers the fundamental question "Why do we need network security?" by examining the potential threats to an enterprise network. It examines network security challenges and the three primary reasons for network security vulnerabilities. It also provides a snapshot of network intruders and addresses the four major categories of network security threats and the tools used to execute them.

Chapter 2, "Evaluating a Network Security Policy," examines the economics of protecting the network and outlines the major components of a network security policy. It also summarizes a network security survey conducted by Cisco and contains an exercise in which you evaluate a sample security policy.

Chapter 3, "Securing the Network Infrastructure," presents how to configure Cisco routers to secure the campus network environment. It covers securing the administrative interface, controlling SNMP access to network devices, ways to control routing updates from interlopers, simple methods to control network traffic, and controlling Ethernet switch port and access security.

Part II: Dialup Security

Chapter 4, "Examining Cisco AAA Security Technology," discusses the AAA architecture and technologies associated with it. It presents concepts useful for implementing AAA security solutions available in Cisco products.

Chapter 5, "Configuring the Network Access Server for AAA Security," discusses how to configure a Cisco network access server to allow AAA processes to use a local or remote security database. In addition, it covers how to troubleshoot problems with AAA processes.

Chapter 6, "Configuring CiscoSecure ACS and TACACS+/RADIUS," discusses the features and architecture of CiscoSecure ACS for Microsoft Windows NT and UNIX platforms. In addition, it describes how to configure CiscoSecure ACS for NT to perform AAA functions for Cisco network access servers, focusing on using the TACACS+ protocol.

Part III: Securing the Internet Connection

Chapter 7, "Configuring a Cisco Perimeter Router," presents how to create a perimeter security system using the security features of a Cisco router. It includes an overview of perimeter security components and Cisco IOS software features that are useful for perimeter security. It also shows you how to use each feature to secure the network perimeter.

Chapter 8, "Configuring the Cisco IOS Firewall," discusses how to use the Cisco IOS Firewall feature set on Cisco routers to enhance perimeter security. It includes an overview of context-based access control, and it shows you how to configure the IOS Firewall in a perimeter security system.

Part IV: Configuring the CiscoSecure PIX Firewall

Chapter 9, "PIX Firewall Basics," presents the capabilities, features, and configuration options of the PIX Firewall family. It shows that the PIX Firewall can provide powerful security even with a basic configuration command set.

Chapter 10, "Configuring Access Through the PIX Firewall," builds on Chapter 9, discussing how to control inbound and outbound access through the PIX Firewall with specific configuration commands. It includes configuring network address translation, static translations, and other methods of access control.

Chapter 11, "Configuring Multiple Interfaces and AAA on the PIX Firewall," discusses how to flexibly configure multiple interfaces on the PIX Firewall to create a more-secure DMZ. It also covers how to configure AAA features of the PIX Firewall to work with CiscoSecure ACS, enabling user-level access control.

Chapter 12, "Configuring Advanced PIX Firewall Features," discusses some of the more specialized features of the PIX Firewall that make it a powerful yet flexible firewall to control Internet access and features. It includes coverage of PPTP support, Java applet blocking, URL and FTP filtering, SNMP and syslog support, PIX Firewall redundancy, and maintenance features.

Part V: Configuring Cisco Encryption Technology

Chapter 13, "Cisco Encryption Technology Overview," discusses the concepts required to configure Cisco Encryption Technology on Cisco routers. It presents encryption algorithms, hashing techniques, digital signatures, and key exchange methods used with Cisco Encryption Technology.

Chapter 14, "Configuring Cisco Encryption Technology," presents the tasks and steps you must follow to configure Cisco Encryption Technology on Cisco routers. It presents the Cisco IOS commands used to configure and test Cisco Encryption Technology, organized in the order in which you would enter them to enable this feature.

Part VI: Configuring a VPN with IPSec

Chapter 15, "Understanding Cisco IPSec Support," presents an overview of IPSec and the IPSec protocols available in Cisco products used to create a VPN. Each IPSec protocol is considered. Subsequent chapters provide details on how to configure IPSec support in Cisco products.

Chapter 16, "Configuring Cisco IOS IPSec," discusses how to configure IPSec in Cisco routers for preshared key and RSA encryption authentication in a site-to-site topology. It simplifies the complex process you must follow to configure IPSec by breaking it into discreet tasks and steps.

Chapter 17, "Configuring PIX Firewall IPSec Support," discusses how to configure IPSec in PIX Firewalls for preshared key authentication in a site-to-site topology. It presents how to configure IPSec in tasks and steps, showing you all the commands necessary to enable this feature.

Chapter 18, "Scaling Cisco IPSec Networks," describes how to configure Cisco IPSec networks consisting of Cisco routers and PIX Firewalls using IPSec so that they can scale to support multiple IPSec peers while maintaining security. It covers how to configure certification authority support and remote access for Cisco VPN client access.

Part VII: Appendixes

Appendix A, "XYZ Company Case Study Scenario," describes the XYZ Company case study to help tie together the security concepts and implementation procedures discussed throughout this book. It presents the IP addresses and networking devices used in sample configurations in each chapter.

Appendix B, "An Example of an XYZ Company Network Security Policy," contains an example of a network security policy for the XYZ Company network used throughout this book. It includes policy statements that address major issues of enterprise network security for the XYZ Company.

Appendix C, "Configuring Standard and Extended Access Lists," summarizes Cisco IOS access lists, which are fundamental to many security features in Cisco routers. It includes coverage of commands used with standard and extended IP access lists.

Appendix D, "Answers to Review Questions," provides the answers to the review questions at the end of each chapter.

Contents at a Glance

Contents